An Efficient Trust-Based Routing Scheme by Max-Min Composition of Fuzzy Logic for MANET

Joydeep Kundu, Koushik Majumder and Debashis De

Abstract Mobile ad hoc network is an infrastructure-less network of distributed nodes. It is spontaneous, self-organized, and also dynamic. In ad hoc environment, due to frequent communication among nodes and lack of enough information about nodes, it is complicated to measure trust. It has been observed that the nature of trust is dynamic that means its value varies with respect to time. Therefore, fuzzy logic is the more suitable technique for expressing and computing the node's trust value than other existing probabilistic approach. In this paper, node's trust values are converted into membership function of the fuzzy logic with the help of Gaussian membership function for clustered ad hoc network. Then cluster head is able to obtain the highly trusted nodes by the fuzzy logic-based max-min composition technique for the purpose of successful communication between sources and destination, so that it can be able to identify and save the nodes against non-cooperative nodes efficiently. It saves the energy consumption by avoiding packet delivery to the non-cooperative nodes by selecting the trusted neighbors for the purpose of communication. Therefore, we have been able to design a reliable and better throughput trust routing method for clustered ad hoc network using max-min composition technique of the membership function of fuzzy logic.

Keywords Cluster · Fuzzy logic · Fuzzy membership function · Max-min composition · Trust

Introduction

A mobile ad hoc network is made up of autonomous nodes which are communicated with others in a self-organizing manner. Thus it is a dynamic and infrastructure-less network [1]. The performance of such network depends on the

Joydeep Kundu · Koushik Majumder (✉) · Debashis De
Department of Computer Science and Engineering, West Bengal
University of Technology, Kolkata, West Bengal, India
e-mail: koushik@ieee.org

N. Afzalpulkar et al. (eds.), *Proceedings of the International Conference on Recent Cognizance in Wireless Communication & Image Processing*,
DOI 10.1007/978-81-322-2638-3_50

cooperative and trust nature of the neighborhood nodes. Each node in the network acts as a router and forwards data packets for other nodes. Several trust-based routings have been established but still it demands for newer methods for the purpose of more reliable, robust, simple, and secure routing in MANET. The routing protocols play an important role for transferring data packets. With respect to security, mainly two basic routings such as cryptographic and trust-based mechanism are used in the field of ad hoc environment. Cryptographic techniques are used to protect the data packets which are transmitted in the clustered ad hoc network. The primary goal of the cryptography-based mechanism is to address confidentiality, node's authentication, and integrity of the data for the purpose of information security. But the major problem with the cryptographic techniques is that this technique is computationally intensive and also fails to detect the malicious nodes. Therefore, these techniques are not suitable to be incorporated in the field of ad hoc network which is prone to different types of security vulnerabilities and where constraint of the resources is an important issue. Here, an alternative trust-based mechanism can also be chosen. These schemes are used to provide the trust values of the nodes in order to detect the nodes with malicious intention and thus it secures the data packet transmission from source and destination through trustworthy nodes. The most challenging routing issue in MANET is its dynamic topology due to nodes limited energy, nodes mobility, and the presence of the misbehaving nodes. Therefore, this topology disturbs the presence of current routes among the source and destination. Security mechanisms for wired network cannot be use in MANET due to its infrastructure-less dynamic topology and constraint battery power. Therefore, identifying the malicious nodes in MANET is the most challenging issue. So security solution for MANET routing scheme should satisfy both essential factors in terms of integrity and stability.

This paper contains five sections which are listed below: section "Related Work" of this paper describes a brief about the related work. Methodologies are discussed in section "Methodology". Section "Implementation of Newly Proposed Trust Scheme" explains the detailed description about the fuzzy-based proposed protocol. Finally, section "Conclusion" concludes the paper.

Related Work

Various types of trust-based methods have been developed that focus on different types of performance metrics of the nodes. It has been seen that the nodes in ad hoc network act as a router, so nodes may have complete processing capabilities, e.g., laptops, cell phones, etc. In most of the cases, in terms of secure routing protocols [2] or secure key management protocols [3], the security solutions can be described. Secure key management protocols require high computational overhead on the nodes. But in practice, nodes have limited power in the ad hoc network. Secure routing protocols depend on the trust model for avoiding the congestion within the network and influence them to perform in a self-organizing manner. Thus the total trust measurement within a cluster is obtained by fuzzified the factors like packet delivery ratio and energy factor into our scheme. Some of the existing secure routing protocols are described below. Weighted cluster algorithm (WCA) is proposed for MANET in [4]. WCA chooses the cluster head based on the factors like ability to handle nodes, mobility, communication range, etc. It computes the average weight of every node using these factors. Then the node with minimum weight is elected as a cluster head (CH). K-hop connectivity ID clustering algorithm (KCONID) is described in [5]. According to mechanism, the node whose connectivity is large is selected as a cluster head. If the connectivity values of two cluster members within the same cluster same then KCONID protocol selects the node having lower ID as a CH.

Methodology

(a) *Fundamental concept about fuzzy logic implementation with fuzzy membership function*

In fuzzy logic, the truth value is the essential factor for any type of statements. The truth values of the statements and membership values of the functions are represented by a value within the range [0.0, 1.0] in fuzzy logic and fuzzy sets, respectively, where 0.0 and 1.0 indicate the absolute false and absolute true decision in fuzzy system. The other values within the range can be computed with the help of fuzzy membership function (Gaussian membership function, Triangular membership function). For implementing fuzzy logic into a trust-based model, it must have the characteristics [6]: (a) it takes the trust knowledge from different nodes into its trust score matrix; (b) each node should be able to compute its own trust score; and(c) it should be dependable and robust against a node with malicious intention. There are several fuzzy membership functions [7] used in fuzzy systems. One of the functions has listed below:

Gaussian Membership Function

A Gaussian membership function is represented by (1), where the parameters c and σ are used to compute the center and width of the curve of the membership function:

$$\mathrm{Gaussian}(x : c, \sigma) = e^{-\frac{1}{2}\left(\frac{TR-c}{\sigma}\right)^2} \tag{1}$$

The Gaussian membership function has two-sided membership function, where the first and second functions describe the left and right side curve of the membership function. The left side function represents the left side curve and right side function determines the right side curve. Normally, center of the left side curve is less than the center of the right side curve.

(b) Fuzzy logic-based Max-min composition rule

The basic rules for obtaining the trust scores (high (H), medium (M), low (L)) based on the max-min composition technique are listed below [8], where TR is the set of universe of discourse of the trust values between the ranges 0–50 and *N* is the set of universe of discourse of node ratings between the ranges 1–10 ((1–3, Malicious node), (4–6, Medium trusted node), (7–10, High trusted node)).

Scenario 1

(i) IF trust value is HIGH THEN node is TRUSTED:

$$R_1(TR, N) = (HXT) \cup (\bar{H}XN) \tag{2}$$

(ii) The condition for highly trusted node is

$$R_H = H \circ R_1(TR, N); \tag{3}$$

where '∘' denotes max-min composition.

Scenario 2

(i) IF trust value is MEDIUM THEN node is MEDIUM TRUSTED:

$$R_2(TR, N) = (MXMT) \cup (\bar{M}XN) \tag{4}$$

(ii) The condition for medium trusted node is

$$R_M = H \circ R_2(TR, N); \tag{5}$$

Scenario 3

(i) IF trust value is LOW THEN node is MALICIOUS:

$$R_3(TR, N) = (LXM) \cup (\bar{L}XN) \tag{6}$$

(ii) The condition for Malicious/low trusted node is

$$R_L = H \circ R_3(TR, N); \tag{7}$$

So the general rule of fuzzy logic-based max-min composition for highly trusted nodes is represented below:

$$R_1\,(TR, N)_{50*10} = HXT_{50*10} \cup \bar{H}XT_{50*10}$$

$$R_H = H \circ R_1(TR, N) = H_{1*50} \circ R_{50*11} = R_{1*11}$$

$$\begin{aligned} R_H &= H^{\circ} R_1(TR, N) = H_{1*50}{}^{\circ} R_{50*11} = R_{1*11} \\ &= [\mathrm{Max}\{\min(H_{1,1}, R_{11,1}), \min(H_{1,2}, R_{12,1}), \ldots, \min(H_{1,50}, R_{150,1})\}, \ldots, \\ &\quad \mathrm{Max}\{\min(H_{1,1}, R_{11,50}), \min(H_{1,2}, R_{12,50}), \ldots, \min(H_{1,50}, R_{150,50})] \end{aligned} \tag{8}$$

Implementation of Newly Proposed Trust Scheme

The main objective of the proposed trust-based routing scheme is to send packets successfully through a trusted and energy-efficient route in clustered ad hoc network. Therefore, it is able to discard the non-cooperative node during the time of active route selection. In this protocol, CH calculates the trust score about its all cluster members (CMs) based on the max-min composition of fuzzy logic within its trust score matrix [8, 9]. At first, the source node forwards the 'Hello' message to the cluster head (CH) for discovering the multiple routes to destination. The CH examines if the destination node belongs to its cluster or not. If it is found into the same cluster, then a positive feedback should be sent to the source and source obtains the multiple destination routes through intra-cluster routing. Otherwise, it sends a negative acknowledgement that means the destination does not belong to that cluster. At that time CH of that cluster communicates with its neighbor CH via the gateway nodes for discovering the destination. Whenever the neighbor CH finds the destination within its cluster, it immediately sends the route discovery message to that CH through the gateway nodes either by direct or via neighbor CHs (inter-cluster routing). After finding the multiple routes, source forwards the route-request message to its neighbor cluster members for obtaining the instant values of packet forwarding ratio. Every cluster member computes the packet transmission ratio at its neighbor cluster member [9]. Then these numerical values are converted into the fuzzy membership value by fuzzy membership function (Triangular and Gaussian membership function). Source sends both the values of its neighbor CMs to the CH, and CH then calculates the total trust values of all individual CM within its trust score matrix. It (CH) converts the numerical value of trust scores into fuzzy membership value using max-min composition of fuzzy logic. The membership values of the cluster members are preserved by the CH in the form of matrix dynamically. Finally, CH finds the highly trusted CMs based on the fuzzy logic-based trust computation unit and send a most trusted route discovery message to the source. Thus source establishes a highly trusted route to the destination and transfers the data packets successfully until the better route is obtained.

Conclusion

In this paper we have designed a trust-based routing protocol for clustered-based MANET. The main objective of this routing scheme is to obtain the most reliable path during the time of packet transmission from source to destination. This mechanism is able to avoid the choosing of a malicious node which acts as a genuine node in the field of ad hoc network. This paper explains that how the cluster head computes its trust score matrix according to the fuzzy logic-based max-min composition for the highly trusted nodes. The CH is able to obtain the set of maximum trusted CMs (cluster members) from the participated member nodes using the fuzzy logic-based max-min composition technique. In this trust routing scheme, we consider the max-min composition because it performs better than the other projection of fuzzy relation such as min-max composition, Cartesian product, etc. Thus our enhanced and simple trust evaluation scheme can efficiently detect and protect against malicious nodes.

References

1. Kumar, M., Mishra, R.: An overview of MANET: history, challenges and applications. Indian J. Comput. Sci. Eng. (IJCSE) **3**(1) 2012
2. Zapata, M.G., Asokan, N.: Securing ad hoc routing protocols. In: Proceedings of ACM Workshop on Wireless Security (WiSe ’02), pp. 1–10. ACM Press, Atlanta, USA. Sept 2002. http://doi.acm.org/10.1145/570681.570682
3. Capkun, S., Buttyan, L., Hubaux, J.-P.: Self-organized public-key management for mobile ad hoc networks. In: Proceedings of ACM Workshop on Wireless Security (WiSe ’02), Atlanta, USA, Sept 2002. http://citeseer.nj.nec.com/capkun02selforganized.html
4. Li, X., Yihui, Z.: A new reputation-based trust management strategy for clustered ad hoc networks. In: An International Conference on Networks Security, Wireless Communications and Trusted Computing (2009)
5. Chatterjee, P.: Trust based clustering and secure routing scheme for mobile ad hoc networks. Int. J. Comput. Netw. Commun. (IJCNC), **1**(2) (2009)
6. Luo, j., Liu, X., Zhang, Y., Ye, D., Xu, Z.: Fuzzy trust recommendation based on collaborative filtering for mobile Ad-hoc networks. This work was supported in part by the National Study abroad Scholarship of China under the Grant No. 27U38009 and the NSERC Discovery Fund under the Grant No. 341823-07
7. Banerjee, P.S., Paulchoudhury, J., Bhadra Chaudhuri, S.R.: Fuzzy membership function in a trust based AODV for MANET. Int. J. Comput. Netw. Inf. Secur. **12,** 27–34 (2013). Published Online October 2013 in MECS (http://www.mecs-press.org/). doi:10.5815/ijcnis.2013.12.04
8. Siddique, M.: Fuzzy decision making using max-min method and minimization of regret method (MMR) (720301-P254). June 2009
9. Kundu, J., Majumder, K.: Design of an efficient trust management mechanism for cluster based MANET using beta reputation rating. In: Elsevier Science and Technology Publication Under the Book Series Computer Communication Networks, pp 105–113. ISBN: 9789351072539